J. Symbolic Computation (1998) **26**, 433–444
Article No. sy980222

Reduced Gröbner Bases Under Composition

JAIME GUTIERREZ† AND ROSARIO RUBIO SAN MIGUEL‡

Departamento de Matemáticas, Estadística y Computación,
Universidad de Cantabria, Santander 39071, Spain

In this paper we contribute with one main result to the interesting problem initiated by Hong (1998, J. Symb. Comput. **25**, 643–663) on the behaviour of Gröbner bases under composition of polynomials. Polynomial composition is the operation of replacing the variables of a polynomial with other polynomials. The main question of this paper is: *When does composition commute with reduced Gröbner bases computation under the same term ordering?* We give a complete answer for this question: let Θ be a polynomial map, then for every reduced Gröbner basis G, $G \circ \Theta$ is a reduced Gröbner basis if and only if the composition by Θ is compatible with the term ordering and Θ is a list of permuted univariate and monic polynomials. Besides, we also include other minor results concerned with this problem; in particular, we provide a sufficient condition to determine when composition commutes with reduced Gröbner bases computation (possibly) under different term ordering.

1. Introduction

In two recent papers Hoon Hong addressed the problem of the behaviour of Gröbner bases under composition of polynomials (see Hong (1996, 1998)). This problem can be stated as follows:

Let G be a Gröbner basis–under some term ordering– of the ideal generated by F, where F is a finite set of polynomials in the variables $x_1, \ldots, x_n$; let Θ be a polynomial map, that is, $\Theta = (\theta_1, \ldots, \theta_n)$ is a list of n polynomials in the variables $x_1, \ldots, x_n$. Now, we consider two new polynomial sets: F^* and G^*, obtained from F and G, respectively, by replacing x_i with θ_i. A natural question that arises is:*Is G^* a Gröbner basis of the ideal generated by F^* under the same term ordering?* This is not always true, one can easily find a counter-example (for instance, try to permute variables with the lexicographic order). Then, the next question is: *Under which circumstances G^* is a Gröbner basis of F^*?* In other words, when does Gröbner bases computation commute with composition under the same term ordering? Hong (1998) gave a complete answer: this happens if and only if the composition is "compatible" with the term ordering and the indivisibility (see Section 2).

The main question of this paper is: When does *reduced* Gröbner bases computation commute with composition under the same term ordering?

†E-mail: sarito@matesco.unican.es
‡E-mail: jaime@matesco.unican.es

0747–7171/98/100433 + 12 $30.00/0

In this paper, we give a complete answer. We show that reduced Gröbner bases computation commutes with composition under the same ordering if and only if the composition by Θ is "compatible" with the term ordering and Θ is a list of permuted univariate and monic polynomials. This question appears in Hong (1998) as an open problem, the author makes the following comment about this: 'An answer to this question will shed a new light on the notion of 'reduced'. At this point, we must comment that this question (see Theorem 3.1) is inherently different to the first one (see Theorem 2.2).

Another related and, in a sense, more general problem is: *When does Gröbner bases computation commute with composition under some term ordering (possibly different term ordering)?* Hong (1996) gave a sufficient condition for this last question: this happens if the leading terms of the composition polynomials form a "permuted powering", see Theorem 5.1. We also provide a sufficient condition to determine when composition commutes with reduced Gröbner bases computation (possibly) under different term ordering.

Finally, we would like to remark that polynomial composition is an important and interesting operation with a large number of applications in physics and mathematics. In fact, we often work with a list of polynomials where the variables are defined in terms of other variables. The paper has two natural applications. One of them is in the computation of reduced Gröbner bases of the ideal generated by composed polynomials: so, in order to compute a reduced Gröbner basis of F^*, we first compute a reduced Gröbner basis G of F and carry out the composition on G, obtaining a reduced Gröbner basis of F^*. This seems more efficient than computing a reduced Gröbner basis of F^* directly. On the other hand, the opposite application is decomposing the input polynomial and then applying the method described above. Efficient methods for univariate polynomial decomposition can be seen in Barton and Zippel (1985), Kozen and Landau (1989), Gutierrez *et al.* (1989) and Binder (1996). The algorithm in Gutierrez *et al.* (1989) requires, in the dense representation of a polynomial $f(x)$ of degree n, a total of $O(n^2)$ arithmetic operations in the ground field. Algorithms to decompose multivariate polynomials can be seen in Gutierrez *et al.* (1991) and von zur Gathen (1990). Gathen's method can be performed with $O(mn(n+1)^m Logn)$ operations, where m is the number of variables and n is the total degree of the multivariate polynomial $f(x_1, \ldots, x_m)$.

The paper is divided into six sections. In Section 2, we briefly review the terminology of reduced Gröbner bases theory and some results about the behaviour of Gröbner bases under polynomial composition. These results will be used throughout the subsequent sections. In Section 3, we give a precise statement of the main theorem of this paper. Then, Section 4 shows a proof of the main theorem. We also provide in this section a necessary and sufficient condition to determine when composition commutes with minimal Gröbner bases. In Section 5, we provide a sufficient condition for the reduced Gröbner bases commutation under composition of polynomials with respect different term ordering. Finally, in Section 6, we illustrate the use of our results with several examples of compatible compositions.

2. Gröbner Bases and Composition of Polynomials

2.1. Review of Gröbner bases theory

In this subsection, we introduce some basic terminology and results of Gröbner bases theory for later use. The details (and proofs) can be found in the original papers

(Buchberger (1965, 1985)) or the textbooks (Cox *et al.* (1992) and Becker and Weispfenning (1993)).

NOTATIONS/DEFINITIONS 2.1.

K	*a field.*
a, b, c	*an element of* K.
p, q, r	*a term, that is,* $x_1^{e_1} \cdots x_n^{e_n}$ *for some* $e_1, \ldots, e_n \in \mathbb{N}$.
f, g	*a non-zero polynomial in* $K[x_1, \ldots, x_n]$.
$deg_{x_i}(f)$	*the degree of* f *with respect to the variable* x_i.
F, G	*a non-empty finite set of non-zero polynomials in* $K[x_1, \ldots, x_n]$.
H	*a non-empty (possibly infinite) set of (possibly zero) polynomials in* $K[x_1, \cdots, x_n]$.
$F - G$	*the set of polynomials in* F *which don't belong to* G.
$\mid$	*the divisibility relation over terms, that is,* $p \mid q$ *iff* p *divides* q.
$\nmid$	*the indivisibility relation over terms, that is,* $p \nmid q$ *iff* p *does not divide* q.
$>$	*an admissible term ordering.*
$\mathrm{lc}(f)$	*the leading coefficient of* f *under* $>$.
$\mathrm{lt}(f)$	*the leading term of* f *under* $>$.
$\mathrm{lm}(h)$	*the leading monomial of* h *under* $>$, *that is,* $\mathrm{lm}(h) = \mathrm{lc}(h)\ \mathrm{lt}(h)$ *for* $h \neq 0, \mathrm{lm}(0) = 0$.
$\mathrm{lm}(H)$	*the set* $\{\mathrm{lm}(h) \mid h \in H\}$.
$\mathrm{Ideal}(H)$	*the ideal generated by* H, *that is, the set* $\left\{\sum_i \hat{h}_i h_i \mid h_i \in H\right\}$.
$\mathrm{lcm}(p, q)$	*the least common multiple of* p *and* q.
$\sigma(f, g)$	$\mathrm{lcm}(\mathrm{lt}(f), \mathrm{lt}(g))/\mathrm{lm}(f)$.
$\mathrm{S}(f, g)$	*the* S*-polynomial of* f *and* g, *that is,* $\sigma(f, g)f - \sigma(g, f)g$.
$\overline{f}^F$	*a normal form of* f *with respect to the set* F.

NOTATIONS/DEFINITIONS 2.2.

$\mathrm{GB}(G)$	*the predicate stating that* G *is a Gröbner basis, that is,* $\diamond\ \mathrm{Ideal}(\mathrm{lm}(G)) = \mathrm{Ideal}(\mathrm{lm}(\mathrm{Ideal}(G)))$.
$\mathrm{GB}(G, F)$	*the predicate stating that* G *is a Gröbner basis of* $\mathrm{Ideal}(F)$, *that is,* $\diamond \mathrm{GB}(G)$, $\diamond\ \mathrm{Ideal}(G) = \mathrm{Ideal}(F)$.
$\mathrm{GB}(G)^M$	*the predicate stating that* G *is a minimal Gröbner basis, that is,* $\diamond \mathrm{GB}(G)$, $\diamond\ \forall f \in G,\ \mathrm{lc}(f) = 1$, $\diamond\ \forall f \in G,\ \mathrm{lm}(f) \notin \mathrm{Ideal}(\mathrm{lm}(G - \{f\}))$.
$\mathrm{GB}(G, F)^M$	*the predicate stating that* G *is a minimal Gröbner basis of* $\mathrm{Ideal}(F)$, *that is,* $\diamond\ \mathrm{GB}(G)^M$, $\diamond\ \mathrm{Ideal}(G) = \mathrm{Ideal}(F)$.
F^R	*the predicate stating that* F *is a reduced set, that is,* $\diamond\ \forall f \in F,\ \mathrm{lc}(f) = 1$, $\diamond\ \forall f \in F$, *no term of* f *lies in* $\mathrm{Ideal}(\mathrm{lm}(F - \{f\}))$.
$GB(G)^R$	*the predicate stating that* G *is a reduced Gröbner basis, that is,* $\diamond\ \mathrm{GB}(G)$, $\diamond\ G^R$.

$\mathrm{GB}(G,F)^R$ *the predicate stating that* G *is the reduced Gröbner basis of* $\mathrm{Ideal}(F)$*, that is,*
$\diamond\ \mathrm{GB}(G)^R$,
$\diamond\ \mathrm{Ideal}(G) = \mathrm{Ideal}(F)$.

The following theorem describes the fundamental characterization of the Gröbner bases.

Theorem 2.1. (Buchberger, 1965) *The following are equivalent:*

(A) $\mathrm{GB}(G)$.
(B) $\forall f, g \in G, \overline{\mathrm{S}(f,g)}^{G} = 0$.

2.2. Gröbner bases under polynomial composition

We will use the following notation:

Notations/Definitions 2.3.

Θ	*a list* $(\theta_1, \ldots, \theta_n)$ *of* n *non-zero polynomials in* $K[x_1, \ldots, x_n]$.
$\mathrm{lc}(\Theta)$	*the list* $(\mathrm{lc}(\theta_1), \ldots, \mathrm{lc}(\theta_n))$.
$\mathrm{lt}(\Theta)$	*the list* $(\mathrm{lt}(\theta_1), \ldots, \mathrm{lt}(\theta_n))$.
$\mathrm{lm}(\Theta)$	*the list* $(\mathrm{lm}(\theta_1), \ldots, \mathrm{lm}(\theta_n))$.

Definition 2.4. (Composition) *The composition of* h *by* Θ*, written as* $h \circ \Theta$*, is the polynomial obtained from* h *by replacing each* x_i *in it with* θ_i*. Likewise,* $H \circ \Theta$ *is the set* $\{h \circ \Theta | h \in H\}$.

The following proposition states some basic properties about composition and leading monomials/terms. These will be used throughout the paper.

Proposition 2.1. **(a)** $(fg) \circ \Theta = (f \circ \Theta) \cdot (g \circ \Theta)$.
(b) $(f+g) \circ \Theta = f \circ \Theta + g \circ \Theta$.
(c) $\mathrm{lt}(p \circ \Theta) = p \circ \mathrm{lt}(\Theta)$.
(d) $\mathrm{lm}(p \circ \Theta) = p \circ \mathrm{lm}(\Theta)$.
(e) $\mathrm{lm}(ag \circ \Theta) = a \cdot \mathrm{lm}(g \circ \Theta)$.

Proof. Immediate from their definitions.

The following definitions and results appear in Hong (1998). For more details, the reader can glance through the original paper.

Definition 2.5. (Commutativity with composition) *We say that the composition by* Θ *commutes with Gröbner bases computation iff the following formula is true for* Θ*:*

$$\forall F \forall G[\mathrm{GB}(G,F) \Longrightarrow \mathrm{GB}(G \circ \Theta, F \circ \Theta)].$$

In a similar way, we also define the commutativity of minimal and reduced Gröbner bases with composition. On the other hand, it is very easy to check that the composition by Θ commutes with Gröbner bases computation iff the following formula is true for Θ:

$$\forall G[\mathrm{GB}(G) \Longrightarrow \mathrm{GB}(G \circ \Theta)].$$

Definition 2.6. (Compatibility with term ordering) *We say that the composition by Θ is compatible with a term ordering $>$ iff for all terms p and q, we have*

$$p > q \Longrightarrow p \circ \mathrm{lt}(\Theta) > q \circ \mathrm{lt}(\Theta).$$

The following lemma, which appears in Hong (1996, 1998) papers, states that a composition operation commutes with a leading term extraction if it is compatible with the term ordering. This result will be used throughout the paper.

Lemma 2.1. *If the composition by Θ is compatible with the term ordering $>$ then, for every f, we have:*

(a) $\mathrm{lt}(f \circ \Theta)=\mathrm{lt}(f)\circ\mathrm{lt}(\Theta)$.
(b) $\mathrm{lm}(f \circ \Theta)=\mathrm{lm}(f)\circ\mathrm{lm}(\Theta)$.
(c) If $\mathrm{lc}(\Theta)=(1,\ldots,1)$ *and* $\mathrm{lc}(f)=1$ *then* $\mathrm{lc}(f \circ \Theta) = 1$.

Proof. The proofs of (a) and (b) can be found in Hong (1998). And (c) is immediate from (a) and (b).

Definition 2.7. (Compatibility with indivisibility) *We say that the composition by Θ is compatible with indivisibility iff for all terms p and q, we have*

$$p \nmid q \Longrightarrow p \circ \mathrm{lt}(\Theta) \nmid q \circ \mathrm{lt}(\Theta).$$

We will also use the next result about the indivisibility of term orderings.

Proposition 2.2. (Hong, 1998) *The composition by Θ is compatible with the indivisibility iff the list* $\mathrm{lt}(\Theta)$ *is a 'permuted powering', that is,* $\mathrm{lt}(\Theta)=(x_{\pi_1}^{\lambda_1},\ldots,x_{\pi_n}^{\lambda_n})$, *where* $\pi_j = \pi(j)$ *for* $j \in \{1,\ldots,n\}$, π *is a permutation of* $(1,\ldots,n)$, *and* $\lambda_1,\ldots,\lambda_n > 0$.

The main result in Hong (1998) is:

Theorem 2.2. (Hong, 1998) *The following are equivalent:*

(A) *The composition by Θ commutes with Gröbner bases computation.*
(B) *The composition by Θ is*

(a) compatible with the term ordering $>$ and
(b) compatible with the indivisibility.

The reader who is not familiar with this theorem is encouraged to glance through Hong's work in order to become so.

3. Main Result

This short section is devoted to elaborating on the main result described in the introduction.

Definition 3.1. *We say that Θ is a list of permuted univariate and monic polynomials if and only if $\Theta = (f_1(x_{\pi_1}), \ldots, f_n(x_{\pi_n}))$ where $\mathrm{lm}(f_i){=}x_{\pi_i}^{\lambda_i}$ with $\pi_j = \pi(j)$ for $j \in \{1, \ldots, n\}$, π a permutation of $(1, \ldots, n)$, and $\lambda_1, \ldots, \lambda_n > 0$.*

Now, the main result reads as follows:

Theorem 3.1. (Main theorem) *The following are equivalent:*

(A) *The composition by Θ commutes with reduced Gröbner bases computation.*
(B) *The term ordering $>$ and Θ satisfies*

(a) the composition by Θ is compatible with the term ordering $>$ and
(b) Θ is a list of permuted univariate and monic polynomials.

We will suppose that the number of variables is greater than one, that is, $n \geq 2$. The statement for the case $n = 1$ is a triviality.

4. Proof

This section is mainly dedicated to showing a proof of the theorem stated in the previous one. The proof will be divided into several results which are interesting on their own. At the end of the section, we also provide a necessary and sufficient condition to determine when composition commutes with minimal Gröbner bases computation.

4.1. reduced sets under composition

Here, we study the behaviour of reduced sets under composition of polynomials. We define the commutativity with composition of reduced sets as follows:

Definition 4.1. *We say that the composition by Θ commutes with reduced sets computation iff the following formula is true for Θ:*

$$\forall F[\mathrm{F}^{\mathrm{R}} \Longrightarrow (\mathrm{F} \circ \Theta)^{\mathrm{R}}].$$

Lemma 4.1. *If the composition by Θ commutes with reduced sets, then Θ is compatible with the indivisibility.*

Proof. Let p and q be two terms such that $p \nmid q$. We distinguish two possibilities:

(a) If q does not divide p, then $F = \{p, q\}$ is a reduced set. By hypothesis, we have $F \circ \Theta$ is a reduced set, therefore $p \circ \mathrm{lt}(\Theta) \nmid q \circ \mathrm{lt}(\Theta)$.

(b) If q divides p, then $p = rq$ for some term $r \neq 1$. By Proposition 2.1, we have $p \circ \Theta = (r \circ \Theta)(q \circ \Theta)$. We claim $r \circ \Theta \neq 1$:

Suppose $r \circ \Theta = 1$, then we can choose a term s such that $\{r, s\}$ is a reduced set. By hypothesis, we have $\{r \circ \Theta, s \circ \Theta\} = \{1, s \circ \Theta\}$ is a reduced set. Contradiction.

Thus $p \circ \mathrm{lt}(\Theta) \neq q \circ \mathrm{lt}(\Theta)$ and $q \circ \mathrm{lt}(\Theta)$ divides $p \circ \mathrm{lt}(\Theta)$, therefore $p \circ \mathrm{lt}(\Theta) \nmid q \circ \mathrm{lt}(\Theta)$.

The next result is one of the key tools for the proof of the main theorem:

PROPOSITION 4.1. *The following are equivalent:*

(A) *The composition by* Θ *commutes with reduced sets computation.*
(B) Θ *is a list of permuted univariate and monic polynomials.*

PROOF.
(A) $\Longrightarrow$ **(B)**: By the above Lemma 4.1 and Proposition 2.2, we know that $\mathrm{lt}(\Theta) = (x_{\pi_1}^{\lambda_1}, \ldots, x_{\pi_n}^{\lambda_n})$ where $\pi_j = \pi(j)$ for $j \in \{1, \ldots, n\}$ and $\lambda_1, \ldots, \lambda_n > 0$. Let $i \in \{1, \ldots, n\}$. Thus, we have to prove that θ_i is a univariate and monic polynomial in x_{π_i}.

Let $j \in \{1, \ldots, n\}$ such that $j \neq \pi_i$. There exists j' such that $\pi_{j'} = j$. We consider the set $F = \{x_{j'}, x_i^{\lambda_{j'}}\}$. F is a reduced set, as $i \neq j'$ ($\pi_{j'} = j \neq \pi_i \Rightarrow i \neq j'$). By hypothesis $F \circ \Theta = \{\theta_{j'}, \theta_i^{\lambda_{j'}}\}$ is a reduced set. Therefore, $\mathrm{lt}(\theta_{j'}) = x_j^{\lambda_{j'}}$ does not divide any term of $\theta_i^{\lambda_{j'}}$. This implies that

$$deg_{x_j}(\theta_i^{\lambda_{j'}}) < \lambda_{j'}.$$

This is possible only when $deg_{x_j}(\theta_i^{\lambda_{j'}}) = 0$. Therefore, θ_i is a univariate polynomial in the variable x_{π_i}.

Finally, $F = \{x_i\}$ is always a reduced set. Then, $F \circ \Theta = \{\theta_i\}$ is also a reduced set, which implies that $\mathrm{lc}(\theta_i) = 1$.

(B) $\Longrightarrow$ **(A):**

Reciprocally, suppose Θ is a list of permuted univariate and monic polynomials. Let F be a reduced set. For $f \in F$, let p be a term of f and let $g \in F - \{f\}$. We claim that $\mathrm{lt}(g \circ \Theta) \nmid \mathrm{lt}(p \circ \Theta)$:

As F is a reduced set, we have $\mathrm{lt}(g) \nmid p$. On the other hand, the composition by Θ is compatible with the indivisibility so $\mathrm{lt}(g \circ \Theta) = \mathrm{lt}(g) \circ \mathrm{lt}(\Theta) \nmid p \circ \mathrm{lt}(\Theta) = \mathrm{lt}(p \circ \Theta)$.

Next, we are going to analyse $p \circ \Theta$. We write $\mathrm{lt}(g \circ \Theta) = x_{\pi_1}^{\alpha_1} \cdots x_{\pi_n}^{\alpha_n}$ and $p = x_1^{\beta_1} \cdots x_n^{\beta_n}$. Thus, $p \circ \Theta = f_1(x_{\pi_1})^{\beta_1} \cdots f_n(x_{\pi_n})^{\beta_n}$. From Proposition 2.1, we have that $\mathrm{lt}(p \circ \Theta) = p \circ \mathrm{lt}(\Theta) = p \circ (x_{\pi_1}^{\lambda_1}, \ldots, x_{\pi_n}^{\lambda_n}) = x_{\pi_1}^{\lambda_1 \beta_1} \cdots x_{\pi_n}^{\lambda_n \beta_n}$. We know that $\mathrm{lt}(g \circ \Theta) \nmid \mathrm{lt}(p \circ \Theta)$, that is, $x_{\pi_1}^{\alpha_1} \cdots x_{\pi_n}^{\alpha_n} \nmid x_{\pi_1}^{\lambda_1 \beta_1} \cdots x_{\pi_n}^{\lambda_n \beta_n}$. Therefore, there exists $i \in \{1, \ldots, n\}$ such that $\alpha_i > \lambda_i \beta_i$. As $\mathrm{lt}(p \circ \Theta) = x_{\pi_1}^{\lambda_1 \beta_1} \cdots x_{\pi_n}^{\lambda_n \beta_n}$, any term of $p \circ \Theta$ has the following form: $x_{\pi_1}^{\gamma_1 \beta_1} \cdots x_{\pi_n}^{\gamma_n \beta_n}$ where $0 \leq \gamma_j \leq \lambda_j, \forall j$. Thus, $\alpha_i > \lambda_i \beta_i \geq \gamma_i \beta_i$ which implies $x_{\pi_1}^{\alpha_1} \cdots x_{\pi_n}^{\alpha_n} \nmid x_{\pi_1}^{\gamma_1 \beta_1} \cdots x_{\pi_n}^{\gamma_n \beta_n}$.

We have just proved that $\mathrm{lt}(g \circ \Theta)$ does not divide any term of $p \circ \Theta$, and p is an arbitrary term of f. Therefore, $\mathrm{lt}(g \circ \Theta)$ does not divide any term of $f \circ \Theta$ and by Lemma 2.1, $\mathrm{lc}(g \circ \Theta) = 1$. So, $F \circ \Theta$ is a reduced set.

4.2. PROOF OF SUFFICIENCY

We prove the sufficiency of the compatibility condition for commutativity:

Let G be a reduced Gröbner basis, we have to prove that $G \circ \Theta$ is also a reduced Gröbner basis.

On one hand, we have that G is a Gröbner basis and Θ and $>$ satisfy the condition **(B)** of the Theorem 2.2. Thus, $G \circ \Theta$ is a Gröbner basis.

On the other hand, G is a reduced set, then by Proposition 4.1, $G \circ \Theta$ is also a reduced set. That is, $G \circ \Theta$ is a reduced Gröbner basis.

4.3. PROOF OF NECESSITY

In this subsection, we prove the necessity of the compatibility condition for commutativity, that is, we prove that **(A)** implies **(B)**. By Proposition 4.1, we have proved one half of the necessity condition. Now, let us work on the other half: the commutativity with reduced Gröbner bases computation implies the compatibility with the term ordering.

LEMMA 4.2. *If the composition by Θ commutes with reduced Gröbner bases computation then Θ is compatible with the term ordering.*

PROOF. We will prove this result for two different cases.

(a) In the first case, we take two terms p and q, such that $p > q$ and $q|p$. Therefore, there exists a term $s \neq 1$ such that $p = sq$. From Lemma 4.1 and Proposition 2.2, $\mathrm{lt}(\Theta) = (x_{\pi_1}^{\lambda_1}, \ldots, x_{\pi_n}^{\lambda_n})$ where $\pi_j = \pi(j)$ for $j \in \{1, \ldots, n\}$ and $\lambda_1, \ldots, \lambda_n > 0$. Thus $s \circ \mathrm{lt}(\Theta) \neq 1$, that is, $s \circ \mathrm{lt}(\Theta) > 1$. Thereby, $q \circ \mathrm{lt}(\Theta) < s \circ \mathrm{lt}(\Theta) \cdot q \circ \mathrm{lt}(\Theta) = sq \circ \mathrm{lt}(\Theta) = p \circ \mathrm{lt}(\Theta)$.

(b) For the second case, we take two terms p and q, such that $p > q$ and $q \nmid p$. We also have that $p \nmid q$, because $>$ is an admissible term ordering.

We can write, $p = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ and $q = x_1^{\beta_1} \cdots x_n^{\beta_n}$. Let $I = \{i \in \{1, \ldots, n\} : \beta_i < \alpha_i\}$ and $J = \{j \in \{1, \cdots, n\} : \beta_j \geq \alpha_j\}$. As $p \nmid q$ and $q \nmid p$, $I \neq \emptyset$ and $J \neq \emptyset$.

We rewrite any term $x^a = x_1^{a_1} \ldots x_n^{a_n}$ as follows: $x^a = y^{a_y} z^{a_z}$, where $y^{a_y} = \prod_{i \in I} x_i^{a_i}$ and $z^{a_z} = \prod_{j \in J} x_j^{a_j}$. Then, $p = y^{\alpha_y} z^{\alpha_z}$ and $q = y^{\beta_y} z^{\beta_z}$.

Next, we define $r = x_1^{\gamma_1} \ldots x_n^{\gamma_n} = y^{\gamma_y} z^{\gamma_z}$ where $\gamma_i = \beta_i$ if $i \in I$ and $\gamma_j = 2\beta_j - \alpha_j$ if $j \in J$, that is, $r = y^{\beta_y} z^{2\beta_z - \alpha_z}$.

Let $G = \{p + q, r\}$. We claim that G is a reduced Gröbner basis:

GB(G):

In order to prove it, we will see that $\overline{\mathrm{S}(p+q, r)}^{G} = 0$ (see Theorem 2.1).

$\mathrm{lcm}(\mathrm{lt}(p+q), \mathrm{lt}(r)) = \mathrm{lcm}(p, r) = y^{\alpha_y} z^{2\beta_z - \alpha_z}$ due to in $I, \beta_i < \alpha_i$ and in $J, \beta_j \geq \alpha_j \Rightarrow 2\beta_j - \alpha_j \geq \beta_j \geq \alpha_j$.

$$\begin{aligned}
\mathrm{S}(p+q, r) &= \frac{\mathrm{lcm}(\mathrm{lt}(p+q), \mathrm{lt}(r))}{\mathrm{lm}(p+q)}(p+q) - \frac{\mathrm{lcm}(\mathrm{lt}(p+q), \mathrm{lt}(r))}{\mathrm{lm}(r)} r \\
&= \frac{\mathrm{lcm}(p, r)}{p}(p+q) - \frac{\mathrm{lcm}(p, r)}{r} r = \frac{\mathrm{lcm}(p, r)}{p} q \\
&= \frac{y^{\alpha_y} z^{2\beta_z - \alpha_z}}{y^{\alpha_y} z^{\alpha_z}} y^{\beta_y} z^{\beta_z} = y^{\beta_y} z^{2\beta_z - \alpha_z} z^{\beta_z - \alpha_z} = r z^{\beta_z - \alpha_z}.
\end{aligned}$$

G^R: On one hand, we have that $q \nmid p$, then there exists $j_0 \in J$ such that $\beta_{j_0} > \alpha_{j_0}$. So $\gamma_{j_0} = 2\beta_{j_0} - \alpha_{j_0} > \beta_{j_0} > \alpha_{j_0}$. This implies that $r \nmid q$ and $r \nmid p$.

On the other hand, $p \nmid q$, then there exists $i_0 \in I$ such that $\alpha_{i_0} > \beta_{i_0}$. So $\gamma_{i_0} = \beta_{i_0} < \alpha_{i_0}$. This implies that $p \nmid r$.

We have just proved that G is a reduced Gröbner basis, and by hypothesis we have that $G \circ \Theta$ is a reduced Gröbner basis.

Finally, we will prove that $\mathrm{lt}((p+q) \circ \Theta) = p \circ \Theta$.

We have that $\mathrm{lt}(p \circ \Theta) = p \circ \mathrm{lt}(\Theta) \neq \mathrm{lt}(q \circ \Theta) = q \circ \mathrm{lt}(\Theta)$. Then, $\mathrm{lt}((p+q) \circ \Theta)$ is equal to $p \circ \mathrm{lt}(\Theta)$ or $q \circ \mathrm{lt}(\Theta)$. Suppose that $\mathrm{lt}((p+q) \circ \Theta) = q \circ \mathrm{lt}(\Theta)$.

Thus, we have that $G \circ \Theta = \{p \circ \Theta + q \circ \Theta, r \circ \Theta\}$ is a reduced Gröbner basis, so

$q \circ \mathrm{lt}(\Theta) \nmid \mathrm{lt}(r \circ \Theta) = r \circ \mathrm{lt}(\Theta)$. That is, $x_{\pi_1}^{\beta_1\lambda_1} \cdots x_{\pi_n}^{\beta_n\lambda_n} \nmid x_{\pi_1}^{\gamma_1\lambda_1} \cdots x_{\pi_n}^{\gamma_n\lambda_n}$. Thus, there exists $k \in \{1, \ldots, n\}$ such that $\lambda_k\beta_k > \lambda_k\gamma_k$, so $\beta_k > \gamma_k$. This is a contradiction, because in I and J, $\gamma_l \geq \beta_l$.

Thereby, $\mathrm{lt}((p+q) \circ \Theta) \neq q \circ \Theta$, so $\mathrm{lt}((p+q) \circ \Theta) = p \circ \Theta$. In other words, $q \circ \mathrm{lt}(\Theta) < p \circ \mathrm{lt}(\Theta)$.

4.4. minimal Gröbner basis under composition

Finally, it is important to point out that Theorems 3.1 and 2.2 are intrinsically different. However, for minimal Gröbner bases we can easily obtain (using Hong's result) that the minimal Gröbner bases computation commutes with composition if and only if the composition is compatible with the term ordering and the indivisibility (exactly as in Theorem 2.2) and $\mathrm{lc}(\Theta) = (1, \ldots, 1)$:

Proposition 4.2. *The following are equivalent:*

(A) *The composition by* Θ *commutes with Gröbner bases computation and* $\mathrm{lc}(\Theta) = (1, \ldots, 1)$.
(B) *The composition by* Θ *commutes with minimal Gröbner bases computation.*

Proof.
(A) $\Longrightarrow$ **(B)**:
Let $G = \{g_1, \ldots, g_m\}$ be a minimal Gröbner basis. As G is a Gröbner basis, $G \circ \Theta$ is a Gröbner basis. Thus, we only have to prove that $\mathrm{lt}(g_i \circ \Theta) \nmid \mathrm{lt}(g_j \circ \Theta) \forall i \neq j$ and $\mathrm{lc}(g_i \circ \Theta) = 1 \forall i$.

We know that G is a minimal Gröbner basis, therefore for any $i, j \in \{1, \ldots, m\}$ such that $i \neq j$, $\mathrm{lt}(g_i) \nmid \mathrm{lt}(g_j)$. By Theorem 2.2, we have that the composition by Θ is compatible with the indivisibility. Hence, $\mathrm{lt}(g_i \circ \Theta) = \mathrm{lt}(g_i) \circ \mathrm{lt}(\Theta) \nmid \mathrm{lt}(g_j) \circ \mathrm{lt}(\Theta) = \mathrm{lt}(g_j \circ \Theta)$, see Lemma 2.1.

Now, we have that $\mathrm{lc}(g_i)$=1 and $\mathrm{lc}(\Theta)$=$(1, \ldots, 1)$. Again, by Lemma 2.1, $\mathrm{lc}(g_i \circ \Theta)$=1.
(B) $\Longrightarrow$ **(A):**
Let G be a Gröbner basis. Removing elements of G, we can find G' such that $\mathrm{GB}(G', G)$ and $\forall g' \in G', \mathrm{lm}(g') \notin \mathrm{Ideal}(\mathrm{lm}(G' - \{g'\}))$.

We consider the set $G'' = \{g'/\mathrm{lc}(g') | g' \in G'\}$.

Obviously, we have $\mathrm{GB}(G'', G)^M$. Thus, by **(B)**, $\mathrm{GB}(G'' \circ \Theta, G \circ \Theta)^M$.

Now, we note that:

$$\begin{aligned}\mathrm{Ideal}(\mathrm{lm}(G \circ \Theta)) &\supset \mathrm{Ideal}(\mathrm{lm}(G' \circ \Theta)) = \mathrm{Ideal}(\mathrm{lm}(G'' \circ \Theta)) \\ &= \mathrm{Ideal}(\mathrm{lm}(\mathrm{Ideal}(G'' \circ \Theta)) = \mathrm{Ideal}(\mathrm{lm}(\mathrm{Ideal}(G \circ \Theta)).\end{aligned}$$

Therefore, $G \circ \Theta$ is a Gröbner basis.

Finally, for every $i \in \{1, \ldots, n\}$, $\mathrm{GB}(\{x_i\})^M$; so $\mathrm{GB}(\{x_i \circ \Theta = \theta_i\})^M$. Thus, $\mathrm{lc}(\theta_i) = 1$.

5. Reduced Gröbner Bases under Different Term Ordering

This section is devoted to the behaviour of reduced Gröbner bases under composition of polynomials (possibly) under different term orderings.

We start with the notations we will use in this section. As in Hong (1996), we define:

NOTATIONS/DEFINITIONS 5.1. (COMPOSITION ON ORDERING) *The composition of* $>$ *by* Θ*, written as* $\succ\!\!\circ\Theta$*, is the binary relation over the terms defined by*

$$\forall p \forall q [p \succ\!\!\circ\Theta\, q \Longleftrightarrow p \circ \mathrm{lt}(\Theta) > q \circ \mathrm{lt}(\Theta)].$$

We will need to refer to $\succ\!\!\circ\Theta$ *numerous times. So we will use* $>'$ *instead of* $\succ\!\!\circ\Theta$*.*

Note that the relation $>'$ is not necessarily an admissible term ordering. See Lemma 5.1 under which conditions it is.

NOTATION 5.2.

$\mathrm{lc}_{>'}(f)$	*the leading coefficient of* f *under* $>'$*.*
$\mathrm{lt}_{>'}(f)$	*the leading term of* f *under* $>'$*.*
$\mathrm{lm}_{>'}(f)$	*the leading monomial of* f *under* $>'$*.*
$\mathrm{GB}_{>'}(G)$	*the predicate stating that* G *is a Gröbner basis under* $>'$*.*
$\mathrm{GB}_{>'}(G, F)$	*the predicate stating that* G *is a Gröbner basis of* $\mathrm{Ideal}(F)$ *under* $>'$*.*
$\mathrm{GB}_{>'}(G)^M$	*the predicate stating that* G *is a minimal Gröbner basis under* $>'$*.*
$\mathrm{GB}_{>'}(G, F)^M$	*the predicate stating that* G *is a minimal Gröbner basis of* $\mathrm{Ideal}(F)$ *under* $>'$*.*
$\mathrm{GB}_{>'}(G)^R$	*the predicate stating that* G *is a reduced Gröbner basis under* $>'$*.*
$\mathrm{GB}_{>'}(G, F)^R$	*the predicate stating that* G *is the reduced Gröbner basis of* $\mathrm{Ideal}(F)$ *under* $>'$*.*

We will use the next lemma, which states when the above relation $>'$ is an admissible term ordering.

LEMMA 5.1. (HONG, 1996) *Let*

(A) *The list* $\mathrm{lt}(\Theta)$ *is a permuted powering.*
(B) (a) $>'$ *is an admissible term ordering.*
(b) $\forall p, q[\mathrm{lcm}(p \circ \mathrm{lt}(\Theta), q \circ \mathrm{lt}(\Theta)) = \mathrm{lcm}(p, q) \circ \mathrm{lt}(\Theta)]$.
(c) $\mathrm{lm}(f \circ \Theta) = \mathrm{lm}_{>'}(f) \circ \mathrm{lm}(\Theta)$.
(d) $\mathrm{lt}(f \circ \Theta) = \mathrm{lt}_{>'}(f) \circ \mathrm{lt}(\Theta)$.

Then **(A)** $\Longleftrightarrow$ **(B)**.

The following Theorem, which is the main result in Hong (1996), gives a sufficient condition for the behaviour of Gröbner basis (not necessarily a reduced one) under composition with respect different term ordering.

THEOREM 5.1. (HONG, 1996) *If the list* $\mathrm{lt}(\Theta)$ *is a permuted powering then we have that*

$$\forall F \forall G[\mathrm{GB}_{>'}(G, F) \Longrightarrow \mathrm{GB}(G \circ \Theta, F \circ \Theta)].$$

Note that when Θ is compatible with the term ordering $>$, the binary relation $>'$ is exactly $>$. Thus, this theorem is a generalization of one of the implications in Theorem 2.2.

First, we note that there is no additional condition on the compatibility of the composition with minimal Gröbner basis possibly under different term ordering.

REMARK 5.1. *If the list* $\mathrm{lt}(\Theta)$ *is a permuted powering and* $\mathrm{lc}(\Theta) = (1, \ldots, 1)$ *then we have that*

$$\forall F \forall G[GB_{>'}(G,F)^M \Longrightarrow GB(G \circ \Theta, F \circ \Theta)^M].$$

PROOF. Let F and $G = \{g_1, \ldots, g_m\}$ be such that $\mathrm{GB}_{>'}(G,F)^M$. In particular, G is a Gröbner basis of $\mathrm{Ideal}(F)$. By hypothesis and Theorem 5.1, we have that $\mathrm{GB}(G \circ \Theta, F \circ \Theta)$.

On one hand, G is a minimal Gröbner basis under $>'$, therefore for any element g_i in G, we have $\mathrm{lc}_{>'}(g_i) = 1$, that is, $\mathrm{lm}_{>'}(g_i) = \mathrm{lt}_{>'}(g_i)$. From Lemma 5.1, $\mathrm{lm}(g_i \circ \Theta) = \mathrm{lm}_{>'}(g_i) \circ \mathrm{lm}(\Theta) = \mathrm{lt}_{>'}(g_i) \circ \mathrm{lm}(\Theta) = \mathrm{lt}_{>'}(g_i) \circ \mathrm{lt}(\Theta) = \mathrm{lt}(g_i \circ \Theta)$. Therefore, $\mathrm{lc}(g_i \circ \Theta) = 1$.

On the other hand, for any $i, j \in \{1, \ldots, m\}$ such that $i \neq j$, $\mathrm{lt}_{>'}(g_i) \nmid \mathrm{lt}_{>'}(g_j)$. As $\mathrm{lt}(\Theta)$ is a permuted powering, we have that the composition by Θ is compatible with the indivisibility: $\mathrm{lt}_{>'}(g_i) \circ \mathrm{lt}(\Theta) \nmid \mathrm{lt}_{>'}(g_j) \circ \mathrm{lt}(\Theta)$. Using Lemma 5.1 again, we have $\mathrm{lt}(g_i \circ \Theta) \nmid \mathrm{lt}(g_j \circ \Theta)$.

Now, we have enough tools to prove the main result of this section. We will also use some strategies that have been shown in the previous proofs.

THEOREM 5.2. *If* Θ *is a list of permuted univariate and monic polynomials, we have that*

$$\forall F \forall G[\mathrm{GB}_{>'}(G,F)^R \Longrightarrow \mathrm{GB}(G \circ \Theta, F \circ \Theta)^R].$$

PROOF. Let F and G be such that $\mathrm{GB}_{>'}(G,F)^R$. Thus, we have that $\mathrm{GB}_{>'}(G,F)^M$. And Θ satisfies the hypothesis of Remark 5.1, so we obtain that $\mathrm{GB}(G \circ \Theta, F \circ \Theta)^M$.

Let $f \in G$. Let p be a term of f and $g \in G - \{f\}$. As G is a reduced Gröbner basis under $>'$, we have $\mathrm{lt}_{>'}(g) \nmid p$. Moreover, Θ is compatible with the indivisibility, so $\mathrm{lt}(g \circ \Theta) \nmid \mathrm{lt}(p \circ \Theta)$ (see Lemma 5.1).

Next, we analyse $p \circ \Theta$:

Let $\mathrm{lt}(g \circ \Theta) = x_{\pi_1}^{\alpha_1} \cdots x_{\pi_n}^{\alpha_n}$ and $p = x_1^{\beta_1} \cdots x_n^{\beta_n}$. Thus $\mathrm{lt}(p \circ \Theta) = x_{\pi_1}^{\lambda_1 \beta_1} \cdots x_{\pi_n}^{\lambda_n \beta_n}$. As $\mathrm{lt}(g \circ \Theta) = x_{\pi_1}^{\alpha_1} \cdots x_{\pi_n}^{\alpha_n} \nmid \mathrm{lt}(p \circ \Theta) = x_{\pi_1}^{\lambda_1 \beta_1} \cdots x_{\pi_n}^{\lambda_n \beta_n}$, there exists $i \in \{1, \ldots, n\}$ such that $\alpha_i > \lambda_i \beta_i$. As $\mathrm{lt}(p \circ \Theta) = x_{\pi_1}^{\lambda_1 \beta_1} \cdots x_{\pi_n}^{\lambda_n \beta_n}$, any term of $p \circ \Theta$ has the following form: $x_{\pi_1}^{\gamma_1 \beta_1} \cdots x_{\pi_n}^{\gamma_n \beta_n}$ where $0 \leq \gamma_j \leq \lambda_j$ for every j. Thus, $\alpha_i > \lambda_i \beta_i \geq \gamma_i \beta_i$ which implies : $x_{\pi_1}^{\alpha_1} \cdots x_{\pi_n}^{\alpha_n} \nmid x_{\pi_1}^{\gamma_1 \beta_1} \cdots x_{\pi_n}^{\gamma_n \beta_n}$.

We have just proved that $\mathrm{lt}(g \circ \Theta)$ does not divide any term of $p \circ \Theta$, and p is an arbitrary term of f. Therefore, $\mathrm{lt}(g \circ \Theta)$ does not divide any term of $f \circ \Theta$, that is, no term of $f \circ \Theta$ lies in $\mathrm{Ideal}(\mathrm{lm}((G - \{f\}) \circ \Theta))$.

6. Examples of Compatible Compositions

In this section we show some examples of composition with Θ which satisfy the condition of the main results of this paper.

EXAMPLE 6.1. *Let* $>$ *be the lexicographic ordering. Then, every composition of the form* $\Theta = (f_1(x_1), \ldots, f_n(x_n))$ *where* $\mathrm{lm}(f_i) = x_i^{\lambda_i}$ *and* $\lambda_i > 0$ *for every* i*, commutes with reduced Gröbner bases computation.*

EXAMPLE 6.2. *Let* $>$ *be the graded lex ordering. Then, every composition of the form* $\Theta = (f_1(x_1), \ldots, f_n(x_n))$ *where* $\mathrm{lm}(f_i) = x_i^{\lambda}$ *for every* i*, and* $\lambda > 0$*, commutes with reduced Gröbner bases computation.*

EXAMPLE 6.3. *Let $>$ be a term ordering and let $a_1, \ldots, a_n$ be positive and real numbers. We define a term ordering $>_L$ as follows: Let $p = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ and $q = x_1^{\beta_1} \cdots x_n^{\beta_n}$, we define*

$$p >_L q \Longleftrightarrow \begin{cases} a_1\alpha_1 + \cdots + a_n\alpha_n > a_1\beta_1 + \cdots + a_n\beta_n, \\ \text{or} \\ a_1\alpha_1 + \cdots + a_n\alpha_n = a_1\beta_1 + \cdots + a_n\beta_n \text{and} p > q. \end{cases}$$

If Θ is compatible with the term ordering $>$, then every composition of the form $\Theta = (f_1(x_1), \ldots, f_n(x_n))$ where $\mathrm{lm}(f_i) = x_i^{\lambda}$ for every i, and $\lambda > 0$, commutes with reduced Gröbner bases computation. In fact, Example 6.2 is a particular case: taking $a_i = 1, \forall i$ and $>$ the lexicographic ordering.

EXAMPLE 6.4. *Let $>$ be a term ordering ($n = 2$) defined as follows:*
Let $p = x_1^{\alpha_1} x_2^{\alpha_2}$ and $q = x_1^{\beta_1} x_2^{\beta_2}$, we define

$$p > q \Longleftrightarrow \alpha_1 + \sqrt{2}\alpha_2 > \beta_1 + \sqrt{2}\beta_2.$$

Then, every composition of the form $\Theta = (f_1(x_1), f_2(x_2))$ where $\mathrm{lm}(f_i) = x_i^{\lambda}$ for every i, and $\lambda > 0$, commutes with reduced Gröbner bases computation.

Finally, we give one more example illustrating the use of the main results. In this case, it involves a non-trivial permutation of variables.

EXAMPLE 6.5. *Let $>$ be the term ordering defined in Example 6.4. Then, every composition of the form $\Theta = (f_1(x_2), f_2(x_1))$ where $\mathrm{lm}(f_1) = x_2^{\lambda}$ and $\mathrm{lm}(f_2) = x_1^{2\lambda}$ with $\lambda > 0$, commutes with reduced Gröbner bases computation.*

Acknowledgements

We thank the anonymous referees for their valuable comments. This research was done in the framework project FRISCO and PB97-0346.

References

Barton, D., Zippel, R. (1985). Polynomial decomposition algorithms. *J. Symb. Comput.*, **1**, 159–158.
Becker, T., Weispfenning, V. (1993). *Gröbner Bases.* New York–Berlin–Heidelberg, GTM, Springer Verlag.
Binder, F. (1996). Fast Computations in the lattice of polynomial rational function fields. *Proc. ISSAC–96.* Oxford, ACM Press.
Buchberger, B. (1965). Ein algorithmus zum Auffiden der Baiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. Ph D Thesis, Universität Innsbruck, Austria.
Buchberger, B. (1985). Gröbner bases: an algorithmic method in polynomial ideal theory. In Bose, N.K., ed. *Recent Trends in Multidimensional Systems Theory*, D. Reidel.
Cox, D., Little, J., Òshea, D. (1992). *Ideals, Varieties, and Algorithms.* New York–Berlin–Heidelberg, UTM, Springer.
Gutierrez, J., Ruiz De Velasco, C., Recio, T. (1989). A polynomial decomposition algorithm of almost quadratic complexity. *Lect. Notes Comput. Sci.*, 358, pp. 351–356. Berlin, Springer.
Gutierrez, J. (1991). Polynomial decomposition algorithm over factorial Domains. *Comptes Rendues Mathematiques de l'Acad. des Sci.* **XIII**, 81–86.
Hong, H. (1996). Gröbner basis under composition II. *Proc. ISSAC-96.* ACM Press.
Hong, H. (1995). Gröbner basis under composition I. *J. Symb. Comput.*, **25**, 643–663.
Kozen, D., Landau, S. (1989). Polynomial decomposition algorithms. *J. Symb. Comput.*, **7**, 445–456.
von zur Gathen, J. (1990). Functional decomposition of polynomials: the tame case. *J. Symb. Comput.*, **9**, 281–300.

Originally received 28 April 1997
Accepted 1 April 1998